D.O.C.

DEFENDERS OF CRACKING

presents

How to crack a game

Introducing

So you want to be a cracker huh?Aha.I know what do you think.You think i download any shit crack help documents from the internet read them and can start to crack huh?Then i`ll call me CdKiller and be famous as every other cracker in the net huh?NO!!!ALL WHAT YOU HAVE THINK ABOUT CRACKING IS FALSE!!!FORGET IT NOW!!!!CLEAR YOUR BRAIN AND I`LL TEACH YOU HOW TO CRACK!!!!
After you finished reading this text you`ll know how to crack Cd protection and how to disable movie/sound/music calls in the game exe.

WHAT WE NEED TO CRACK

Ok before we can start or let us better say before YOU can start to crack you need an disassembler! I use Win32Dasm and i think its the best prog for crack beginner.
Then you need Hiew to manipulate the exe you want to crack because with Win32Dasm you can only take a look into the exe but you can`t manipulate anything.
Win32Dasm
Hiew
This two things you must called your own to be able to crack progs.
Ok we should think that you have already the two progs and we can start to crack.

LET`S CRACK!!!

Crack with Win32Dasm

Ok in this lesson i`ll show you how to work with Win32Dasm and Hiew.
Today we wanna crack an game which is very easy to crack.We crack Need for Speed 2.
Ok.We start our Win32Dasm.exe.We can see the main page with an toolbar.We click on Disassembler.An menu pops up and we can see some options.We click on Open file to Disassemble.Another pop up menu show us our HD and we click on the exe we want to disassemble(here is it the nfsw.exe).The disassemble process have start the disassembling may take few minutes (be sure that you have over 80MB free space on your HD if not it may be that the exe cannot be fully disassemble).Ok the exe was disassembled.Huh whats that? All what you can see is a text written with WingDings font!NO PROBLEMO AMIGO!!!!
Click on Disassembler and then in the pop up options screen on Font and then on select Font.You can select an Font type (i think the best Font to work with it is Arial).Click on ok.
We can now read the text.Ok.But what the hell all the scurvy things mean?
Object01: Begtext RVA: 00001000 Offset: 00000400 Size: 000AEA00 Flags 60000020
What does it mean?We dont know that.But no matter!We dont need to know that.What we have to do now is to start the game (here Need for Speed 2) without CD.It doesn`t works huh? SHIT!But what does the error message say?
Abort message:
To play Need for Speed 2 you need the Cd
Ok.Now we know the error message!That is very usefull!!!We go back to Win32Dasm (the nfsw.exe is already disassembled) we click right on the toolbar on the button String Data References (it`s the button next to the print button).An pop up window called

Win32Dasm List of String Data Items is now open.Ok.All we have to do is to look for the error message we saw if we start Need for Speed without Cd (To play Need for Speed you need the CD).It beguns with T for "To play" so we dont search at the start but warped to the section where we see the messages that begin with "T".And there is it!The error message "To play Need for Speed 2 you" we doubleclick on the message.We close the pop up menu with the error messages and go back to the main screen of Win32Dasm with the text of the nfsw.exe.We can see that we are not on the beginning of the text but anywhere in the middle.We are now exactly on the place were the error message is.We see some wirrwarr and still don`t know what does it means.But the only thing we must to know is the @offset number of every call or jump command(jump =jmp call = call).We look a moment on the screen and then we see an jump command:
:0044632C EB1BC5E3E1 call 00446349
we use the cursor keys to click on the jump command.The OPbar change his color to green. That means that we can manipulate it (we can manipulate everything in the exe but the green bar show us important commands like jump,call....).We let the bar on the jump command and look below on the bar that show us some numbers:
Line:120246 Pg 1604 of 4273 Code Data @:0045821 @Offset 00045821h in file:nfsw.exe
the only thing we need is number behind @Offset (here is it 00045821)we dont need the last thing h.We write down the number (here 00045821) and close the Win32Dasm window.
We go now to Hiew.

Crack with HIEW

We start the Hiew.exe (h.exe/h95.exe).We can see an list of programms and exes in the HIEW directory it looks like Norten Commander.We use the cursor keys to move up and down and so we go to the directory where we have saved the exe we want to crack (here is it C:\game\nfs2\ nfsw.exe).We click on the exe we want to crack (here nfsw.exe).We see now any wirrwarr and dont know what to do with it.We click F4 and an pop up menu comes.In the pop up menu we click on Decode.Now we can see an list with numbers and other things.We click now on F5 and above on the left site of the screen we can type the number we write down in Win32Dasm (here is it 00045821).We type the number and will be warped by Hiew to the place were the number exist.Now we see any numbers and our cursor is placed on EB1BC5E3E1 (in Need for Speed 2 crack).Ok.Every two numbers means one byte.Here we have EB1BC5E3E1 that means we have 5byte.Now we click on F3 (edit).We can now edit the ten numbers EB1BC5E3E1.We type now 9.If we type we will be warped to an other place but that is no problem.The 9 is still there.We type now an 0 and then again 9 and 0.Thtat we will do for every two numbers that means wo do it 5 times.We click on F9 (update).We have typed five times 90.For every byte 90 for EB=90 1B=90 C5=90 E3=90 E1=90.FOR EVERY BYTE 90.For example: if there stand E8D117FDFF (it is the @offset code for the movie files but no matter now) it means 10 numbers = 5byte and for every byte a 90!!!!The number 90 is the noop number.Ok.We click on F10(quit) we can now run Need for Speed 2 without CD!!!
We have removed the Cd protection for Need for Speed 2!!!!

OK WE DO THAT

Ok we have cracked now the CD protection.

SOMETHING TO REMEMBER

The first thing you have to do if you wanna crack an game is to run the game without CD! Then you look which kind of error message it shows.You must remember the error message and start Win32Dasm then you look under List of String Data Items where you find the error message.
For example: You start the game without movies on your HD.The game may show you an error message like MOVIE FILE not found.Then you look under Win32Dasm where do you find the error message called MOVIE FILE not found.If you find it you doubleclick on it.You can then close the List of Data String Items and go back to the Win32Dasm main screen there you was warped to the place which contain the call or jump commands for the error message.You write down every jump and call @offset number (you recognize the commands if the OPbar change his color to green)you need only the number behind @Offset without the h!!!!Then you go to hiew and type the number in the open field.Then you edit the call or jump command with help of 90 for every byte(remember every two numbers are one byte).Then you click on update and quit.You have now nooped the Game!!!

TROUBLESHOOTING

Q.:What may i do if there are more as one call or jump commands or one call and one jump?
A.:Ok.Now you come to the area where the real cracking begin!One of the call or jump command is an "GOODBOY"and one an"BADBOY"!!!An goodboy is good and if you noop the goodboy it may be to 99% that the game doesnt work.But which of them are good and bad? We dont know that!!!You must experiment!!!The best thing to do is to save the exe and do it on the hard old "try and error"method.You try to noop one then look if the game runs if it`s so great if not you must load your saved exe and try another number.At first you can try to noop every call and jump command you see but i am sure that the game will not run after that.You must experiment with different noops so long as it gets and it works!!!
Q.:There is no String References button avaible!
A.:If it is so it is not good for you!It means that the chance for you to crack the game is 5%. The only thing you can do is to search per hand after keywords like cd/movie/music/error... Or to look under the HexWorkShop if you can find an string you can manipulate.But i thing you`ll have no chance to crack the game.
Q.:I try everything but i cant crack the game!
A.:There are two possible ways:
1.:You do anything wrong if you cracked the game (like noop an GoodBoy,noop anything the game need,noop not enough and dont removed the wanted protection or nooped too much and the game doesnt works)
2.:You cannot crack the game cause the task is too hard or nobody can crack the game (but i think the first thing).

QUICK REMEMBER

-Two numbers are one byte :E4C2A1 means E4=1byte C2=1byte A1=1byte and for every byte a 90 (the noop number)
- Start without Cd then look which kind of error message the game show
- With the message to Win32Dasm and to the String of Data Items pop up menu
- There you have to search where you can find the same error message and double click on it
- Write down the number after @Offset without the h (below the main screen) for every call and jump command (you recognize it if the bar change his color to green)
- Then with the @Offset number to Hiew and noop the address

THAT WAS ALL

I hope you understand my text and are now able to crack gamez and other things!
I know that it is not easy to understand (my gramatic is bader then of an turkish imigrate in russland) but if you try it often enough you`ll check it and crack it!I am sure you do!!!!
This is the first text i write about cracking in my life and i am sure it will be not the last!!!

OUTRO

The text was written by The PuppetMaster2501.I am proud member of one of the newest crack groups called D.O.C. - Defenders of Cracking.If you have some experience in cracking hacking or can program some graphic tools in Turbo Pascal or C++ and wanna be an Defender too and an member of D.O.C. then send me an e-mail and i will contact you.
Lucien91@hotmail.com

ROCK DA PLANET BABY